

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO,
EASTERN DIVISION**

IN THE MATTER OF THE SEARCH OF:

One Apple iPhone 13, bearing serial number)	
D2P9TJ2TD9 and One Apple iPhone 13, bearing)	Case No. 2:22-mj-502
Serial number P9NVHDTD3R, belonging to)	
Joshua GREEN currently held at an offsite office of)	Magistrate Judge
HSI Columbus located at 601 Southgate Pkwy.)	
Cambridge, OH 43725)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Bianca Ragone (Your Affiant), a Special Agent with Homeland Security Investigations (HSI) being duly sworn, hereby depose and state:

I. INTRODUCTION

1. I am a Special Agent (SA) of Homeland Security Investigations (HSI), assigned to the Office of the Assistant Special Agent in Charge, Columbus, Ohio since September 2019. During my tenure as a Special Agent, I have completed the Criminal Investigator Training Program (CITP) and the Homeland Security Investigations Special Agent Training Program (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. During CITP and HSISAT I have received training on cybercrimes, child exploitation, child pornography, and the dark web. I have been assigned to the Franklin County Internet Crimes Against Children (ICAC) Task Force investigating child exploitation offenses since November 2019. Prior to that, I worked for the Federal Bureau of Investigation (FBI) for three years as a Student Work Force Trainee on a Violent Crimes Task Force working child exploitation cases. Moreover, I am a federal law enforcement officer who is engaged in enforcing federal criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, and I am authorized by law to request a search warrant.

II. PURPOSE OF THE AFFIDAVIT

2. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other state and federal law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have not withheld any evidence or information which would negate probable cause. I have set forth only the facts necessary to establish probable cause for a search warrant for the contents of one iPhone 13, bearing serial number D2P9TJ2TD9 seized on February 24, 2022 by Hocking County Sheriff's Office from the residence of Joshua GREEN (GREEN) located at 39642 Poland Road Flushing, OH 43977 (hereinafter referred to as the **SUBJECT DEVICE ONE**) and the contents of one iPhone 13, bearing serial number P9NVHDTD3R seized from GREEN's person on June 21, 2022 at the Belmont County Sheriff's Office pursuant to his arrest (hereinafter referred to as the **SUBJECT DEVICE TWO**), collectively referred to as **SUBJECT DEVICES**. **SUBJECT DEVICES** are currently held in the custody of the HSI Columbus located at 601 Southgate Parkway, Cambridge, Ohio 43725.
3. The **SUBJECT DEVICES** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252, and 2252A – the receipt, possession, and/or distribution of child pornography. I am requesting authority to search the entirety of the **SUBJECT DEVICES**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

4. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
5. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to

knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

6. The term "child pornography"¹, as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.
7. The term "sexually explicit conduct", as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

8. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
9. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
10. “Graphic” when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).
11. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
12. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
13. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
14. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address

² The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

which is used each time the computer accesses the Internet.

15. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, THE INTERNET

16. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
17. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
18. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

19. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.
20. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent

evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses³ and other information both in computer data format and in written record format.
22. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

23. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
24. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
25. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
26. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to

use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a) Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- b) Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications

software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. INVESTIGATION AND PROBABLE CAUSE

29. On June 17, 2022, your affiant received information pertaining to an individual by the name of Joshua E. GREEN, date of birth as February 14, 1981, who was believed to have traded child pornography online after having sustained local convictions for various crimes against children. Specifically, your affiant learned that GREEN was a Tier II registered sex offender currently residing in Flushing, Ohio. Your affiant subsequently obtained numerous reports and spoke with a Special Agent from the Federal Bureau of Investigation (FBI) regarding the FBI investigation of GREEN that had been conducted in the prior months.
30. In or about September of 2021, an FBI Online Covert Employee (OCE) entered a Kik chatroom dedicated to incest and child pornography and engaged in a conversation with Kik user "blueeyes9940" who was later identified as GREEN. During this conversation, the OCE disclosed to GREEN that the OCE was a 12-year-old female, and, at that time, GREEN initiated a private message with OCE via Kik. During GREEN's private messages with the OCE, GREEN distributed numerous images of his nude penis to the OCE along with images of his face. In addition, throughout the course of the conversations between GREEN and the OCE, GREEN requested to know what kind of panties the OCE was wearing.
31. On October 6, 2021, legal process was served on Kik for account information related to "blueeyes9940". In response, Kik noted that the username for the account was "Jay Blue" and the email associated to the account was joshugreen782@yahoo.com³. The registration date for the account was also noted as August 29, 2021.
32. An open-source search for the name "Joshua Green" was then conducted which revealed that there was a Joshua Green in Flushing, Ohio who was a registered sex offender. The

³ Your affiant would note that during an interview with GREEN at a later date, he indicated that this email was a typo and was supposed to be joshuagreen782@yahoo.com.

open-source search also contained a photograph of GREEN. The OCE recognized GREEN from that photo, noting it was the same person depicted in the selfie photographs sent to the OCE by the Kik “blueeyes9940” account. The OCE also learned from the sex offender registry that GREEN worked at 105 Lafayette Ave. Moundsville, West Virginia. Further investigation revealed that located at the 105 Lafayette Avenue address is a Perkins Restaurant & Bakery. Your affiant would note that during GREEN’s chats with the OCE, GREEN stated he was a chef and sent an image of himself in what appeared to be a Perkins t-shirt.

33. In addition to the recovery email for the “blueeyes9940” account, Kik also provided IP logs for the Kik account. A subsequent review of the IP logs indicated that IP address 73.183.7.145 was one of the IP addresses used during the times GREEN was in contact with the OCE. Further open-source searches revealed the above-mentioned IP address was owned and operated by Internet Service Provider (ISP) Comcast Cable. A follow-up subpoena was served on Comcast Cable regarding the above-mentioned IP address and their response indicated the following:

Subscriber Name: Brenda Green

Subscriber Address: 39642 Poland Road Flushing, OH 43977

34. Further open-source research for “Brenda Green” revealed that Brenda still resided at the Flushing, Ohio address with GREEN.
35. On or about February 24, 2022, law enforcement relocated to 39642 Poland Road Flushing, Ohio to attempt a potential interview with GREEN. GREEN was present at the residence and agreed to speak with agents. GREEN indicated that he had previously used Kik for about one to two years but was not active on it anymore. GREEN remembered engaging in a conversation with a 12-year-old girl⁴ via his Kik account and admitted to sending that Kik account pictures of his nude penis. GREEN further admitted to doing this to multiple underaged females via Kik. GREEN further admitted that he had received child pornography of underaged females on Kik but did not remember how many images he had received. He further admitted to being attracted to underaged females and masturbating to

⁴ GREEN was not and is not aware he was speaking to an OCE on Kik. He believed he was talking to a 12-year-old female.

child pornography viewed in the Kik groups. GREEN then consented to the FBI seizing **SUBJECT DEVICE ONE** to conduct a forensic examination on the device.

36. In or about June 2022, your affiant learned that a CyberTipline report was submitted to the National Center for Missing and Exploited Children (NCMEC) on or about January 1, 2022. The CyberTipline report related to the distribution of child pornography from a Kik Messenger account with the username “blackandblue199940”. According to the information that was provided by Kik, between November 25, 2021, and December 2, 2021, approximately nine files depicting child pornography were sent from “blackandblue199940” to another user via Kik private chat message. The CyberTipline report indicated all files were identified using the MD5 hash matching method⁵ but were viewed by the reporting party, Kik. Copies of the uploaded files were included with the CyberTipline report. Your affiant reviewed the files and determined all nine files to be child pornography depicting mostly prepubescent females engaged in sex acts with adult males or masturbation.
37. The CyberTipline also included information pertaining to the IP addresses utilized to access the Kik account at the time the suspect files were transmitted. Your affiant would note that the IP address 73.183.7.145 listed was the same IP address GREEN had utilized when conversing with the OCE via Kik. The CyberTipline provided an email account for the “blackandblue199940” user as joshuagreen782@yahoo.com.
38. In addition to the information noted above, the CyberTipline report also made reference to a second, separate CyberTipline report (Report #105762919) via the NCMEC relating to the same IP address of 73.183.7.145. More specifically, your affiant learned that in February 2022, a subpoena was served to Yahoo, also known as Oath Holdings Inc., by the Ohio Internet Crimes Against Children (ICAC) Task Force relating to the joshugreen782@yahoo.com email address. On or about March 15, 2022, return results

⁵ A hash value is “an algorithmic calculation that yields an alphanumeric value for a file.” *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). Hash values have been referred to as a “unique digital fingerprint,” *United States v. Sosa-Pintor*, 741 Fed. Appx. 207 (5th Cir. 2018), and are “regularly used to compare the contents of two files against each other.” *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). Because only two identical files will return the same hash value, both law enforcement and private cloud storage companies use hash matching to identify and attempt to thwart the spread of child pornography material on the internet. *Id.* at 637-638.

indicated that the email address came back to a Joshua Green with recovery phone number of (740) 338-7402. Further legal process was then served to AT&T, the service provider for the above-mentioned phone number and results from that revealed that the phone was registered to Brenda Bethel, AKA Brenda Green, residing at 39642 Poland Road Flushing, Ohio.

39. Furthermore, your affiant learned that the CyberTipline report (#105762919) was submitted to the NCMEC on or about October 26, 2021 and related to the distribution of child pornography from a Kik Messenger account with the username "blueeyes9940". According to the information that was provided by Kik, on or about October 2, 2021, approximately two files depicting child pornography were sent from the Kik "blueeyes9940" account to another user via private Kik chat messages. The CyberTipline report indicted both files were identified using the MD5 hash matching method again and were originally viewed by the reporting party, Kik. Copies of the uploaded files were included with the CyberTipline report. Your affiant reviewed the files and determined both files to be child pornography which depicted a prepubescent female engaged in acts of masturbation and a prepubescent female, approximately five years of age, engaging in sex acts with an adult male. In addition to the uploaded files, the CyberTipline report also included relevant IP addresses and registration email addresses, both of which again tied back to GREEN.
40. On June 17, 2022, GREEN was arrested by the Belmont County Sheriff's Office (BCSO) on multiple violation of the Ohio Revised Code. During his arrest, **SUBJECT DEVICE TWO** was seized from his person. Pursuant to his arrest, GREEN, after receiving his *Miranda* warnings and agreeing to speak with law enforcement, indicated that no one else had access to **SUBJECT DEVICE TWO** and that any child pornography downloaded to **SUBJECT DEVICE TWO** was from Kik. GREEN admitted that he had viewed child pornography which depicted female(s) in the images/videos as young as 13 years of age. GREEN indicated that he was unsure if any child pornography would be found on **SUBJECT DEVICE TWO** because he deletes the files, further explaining that he would not keep the files long before deleting. GREEN confirmed that prior to deleting images of child pornography off **SUBJECT DEVICE TWO**, he would masturbate to the images/videos. GREEN also confirmed his email account was joshuagreen782@yahoo.com and that one of his Kik accounts was "blackandblue199940". GREEN further admitted that

he would distribute child sexual abuse material in Kik group chats and that he has an addition to child pornography.

41. Your affiant has confirmed that on January 31, 2014, GREEN was convicted of one count of Unlawful Sexual Conduct with a Minor and one count of Pandering Obscenity Involving a Minor in violation of Ohio Revised Code 2907.04(A)(B)(3) and 2907.321(A)(5) out of Belmont County, Ohio. GREEN was sentenced to six months incarceration in Belmont County jail and then six months at the Eastern Ohio Correction Center (EOCC). GREEN was also classified as a Tier II sex offender
42. Based upon the above information, your affiant believes that there is probable cause that **SUBJECT DEVICES** contain additional evidence of child pornography and child exploitation activities.

VII. SEARCH METHODOLOGY TO BE EMPLOYED

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

1. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
2. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
3. Surveying various files, directories and the individual files they contain;
4. Opening files in order to determine their contents;
5. Scanning storage areas;
6. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

7. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

44. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

45. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

- a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure

location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

- d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
 - e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
 - f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.
46. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

47. Based upon the conduct of individuals who have a sexual interest in children and who possess, distribute, and receive child pornography as set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of production, distribution, receipt, and possession of child pornography is currently located on **SUBJECT DEVICES**.


IX. CONCLUSION

48. Based on all the forgoing factual information, there is probable cause to believe that of violations of 18 U.S.C. §§ 2252, and 2252A – the receipt, possession, and/or distribution of child pornography, have been committed and that evidence, fruits and instrumentalities of these offenses will be found within **SUBJECT DEVICES** listed in Attachment A, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of **SUBJECT DEVICES** described in Attachment A, and the seizure of the items described in Attachment B.




Bianca Ragone
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 13th day of July, 2022.



Elizabeth A. Preston Deavers
United States Magistrate Judge



ATTACHMENT A
PROPERTY TO BE TO BE SEARCHED

The devices to be searched are the following:

1. Apple iPhone 13, bearing serial number D2P9TJ2TD9 (**SUBJECT DEVICE ONE**)
2. Apple iPhone 13, bearing serial number P9NVHDTD3R (**SUBJECT DEVICE TWO**)

SUBJECT DEVICE ONE was seized on February 24, 2022 by the Belmont County Sheriff's Office from the residence of Joshua GREEN (GREEN) located at 39642 Poland Road Flushing, OH 43977. **SUBJECT DEVICE TWO** was seized from GREEN's person at the Belmont County Sheriff's Office pursuant to his arrest on June 21, 2022.

SUBJECT DEVICES are currently held in the custody of the HSI Columbus located at offsite office of at 601 Southgate Parkway Cambridge, Ohio 43725.

This warrant authorizes the forensic examination of **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252 and 2252A – the receipt, possession, and/or the distribution of child pornography those violations involving **Joshua GREEN**, including:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography or payments for child pornography or sex trafficking of minors.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse, sexual trafficking of minors, or exploitation of minors.

6. Any and all records, documents, invoices and materials, in any format or medium
(including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.
7. Any and all files, documents, records, or correspondence, in any format or medium
(including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
9. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;
12. Evidence of the utilization of peer-to-peer file sharing programs;
13. Evidence of utilization of user names or aliases, email accounts, social media accounts, and online chat programs, and usernames, passwords, and records related to such accounts;
14. Evidence of software that would allow others to control **SUBJECT DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the

presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;

15. Evidence indicating the computer user's state of mind as it relates to the crimes under investigation;
16. Evidence that **SUBJECT DEVICES** were attached to any other digital device or digital storage medium;
17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from **SUBJECT DEVICES**;
18. Passwords, encryption keys, and other access devices that may be necessary to access **SUBJECT DEVICES**;
19. Records of or information about Internet Protocol addresses used by **SUBJECT DEVICES**;
20. Records of or information about any Internet activity occurring on **SUBJECT DEVICES**, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.